Economic Evaluation of Information Security

El Aoufi, S.

2009

8. Summary

8.1 Research motive

Information Technology (IT) continually places greater demands on an organization to process, maintain, and communicate information. Organizations strongly depend on their information systems, which play a vital role in and make out an important part of their business processes. With the rapid growth of organizations' dependence on information systems, the issue of information security draws more and more attention. There are security breaches, which pose major threats to the reliable execution of business processes, and may have a negative impact on company value, e.g. on profit, shareholder value or reputation. Realizing the rise in security threats, organizations started to invest considerably in information security. While spending on information security has increased, it is still seen as a cost rather than as an investment. Information security still remains hard to sell to business executives. Recent research clarifies that information security is not only a technology problem, but also a matter of economic incentives for information security investment. So the focus is shifting from what is technically possible to what is economically optimal. Organizations have limited resources (fixed budget, etc) for information security investments. Thus, organizations should make resource allocation decisions. However, even if organizations have come to recognize the importance of information security, deciding how much to invest has proved to be challenging. Economics-based research on information security is a relatively new area where researchers examine information security-related problems from a cost-benefit perspective. Since it is a relatively new area, the literature in this stream is scarce.

8.2 Research objective

The objective of the research described in this thesis was specified as follows:

The aim of this research was more economically grounded decisions in information security.

Based on the objective of this research a central research question was formulated. This research question is described in the next section.

8.3 Research problem

The research objective led to the following central question:

How can investments in information security are made in an adequate, economically grounded way?

To find the answer to this question, we defined five sub-questions:

1. *Is it possible to design a method through which investments in information security are made in an adequate, economically grounded way?*
2. *What are the contextual parameters to arrive at more economically grounded investments in information security?*
3. *What data is required to enable the economic evaluation of information security?*
4. *Which process and which process steps should the data undergo to arrive at an economically grounded information security (investment) statement?*
5. *Is the method workable?*

8.4 Research approach

The first step of the research approach was to determine the objective of the research that defined which results needed to be achieved within the research period. This research objective determined the literature and practice to be studied. The research objective led to an overview of the literature concerning information security. The practice study was of a more general nature and provided an insight into the ways in which practice deals with information security investments. Based on the literature study and practice study a method was proposed to assist the business management and the IT management in information security investment decisions. Validating the method was done by performing two activities: *expert review* and *case study*. The process of expert review involved the review of the proposed method elements, i.e., the content, relevance and completeness. Three case studies were performed within different organizations to validate the workability of the method.

8.5 A method to plan the information security investment level

Organizations have to weigh the need for information security against its cost for effective deployment of information security. Since hundred per cent security is rarely feasible in a technical sense and not cost-beneficial in an economic sense, and the organizations have limited resources, organizations need to prioritize information security requirements and thus information security controls. Based on literature study and practice study, a method was proposed to assist business management and IT management in information security investment decisions. In this thesis, a method is a set of steps used to perform a task.

The method links information security requirements to the organization's business processes to determine the appropriate information security investment level. To take the economic aspects of information in consideration, organizations could select the most cost-effective security controls.

The method is designed to help organizations to:

- Prioritize information security requirements;
- Select more cost-effective security controls;
- Perform better evaluations;
- Communicate effectively with the business.

The method consists of three elements, which are summarized below (see Figure 8.1).

- *Context*. The contextual aspects focus on the pressures from within the environment which have an impact on information security. The context responds to the questions:
  - *Why* do organizations implement information security? What are the business drivers?
  - *Who* are the stakeholders?
- *Content*. The content responds to the question:
  - *What* data is relevant and available to facilitate the input of the process? Various techniques can be used to deliver this relevant data.
- *Process*. The process represents the activities to plan the information security investment level. The process responds to the question:
  - *How* is the planning and evaluation of information security investment level performed?

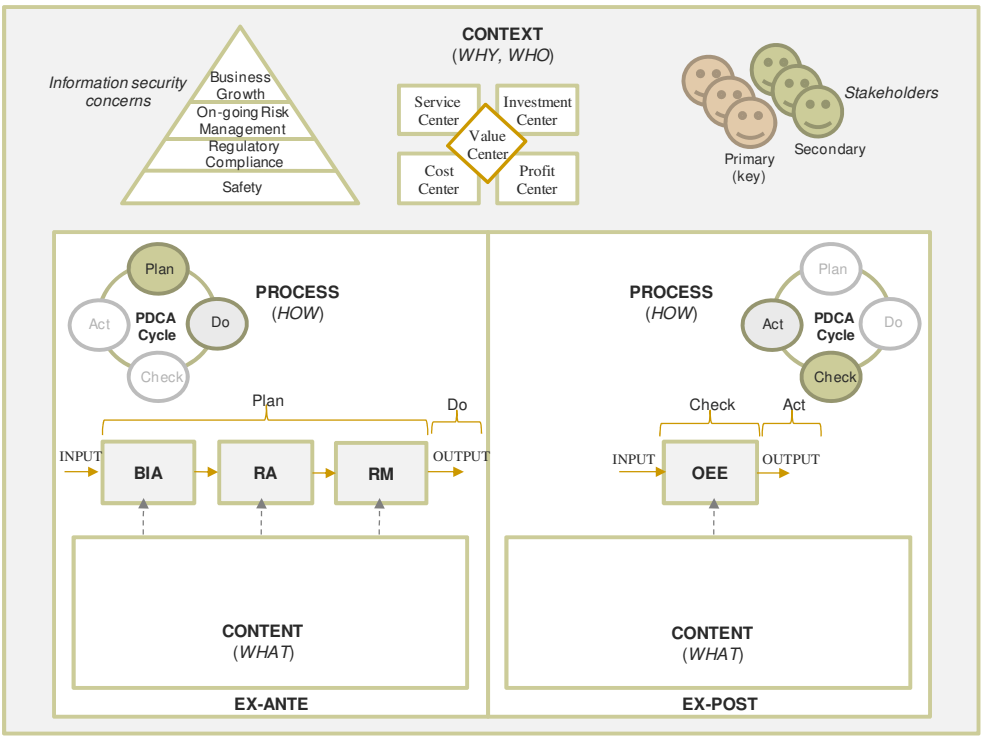

Figure 8.1 The method

The method process consists of two parts: an *ex-ante* part and an *ex-post* part. In the ex-ante part of the method process, information security requirements are determined, prioritized and cost-effective security controls are selected. The results are the service level requirements for information security. Although effectiveness evaluation, the ex-post part, is out of scope of this study, we proposed a decision tree, which can help by evaluating the effectiveness of the implemented information security investment level. The evaluation is necessary to make

sure the service level agreements stay in line with the agreed upon information security level and the possibly changing information security service needs of the business. Further research would involve identifying what the content of the effectiveness evaluation should consist of.

8.6 Research findings

Based on the case studies conducted, the next research findings can be enumerated:

Research finding 1 *It was not easy to find organizations to validate the proposed method. The case study organizations allocated too little time to invest in this research, due to other priorities.*

Research finding 2 *Complying with legislation and regulation was considered to be the top driver for information security within all case study organizations.*

Research finding 3 *The business viewed information security as a Cost Center, the traditional way to manage information security activities within all case study organizations.*

Research finding 4 *The information security maturity level was low within all case study organizations. The organization implemented information security mainly to comply with legislation.*

Research finding 5 *Information security was delivered based on a supply strategy, and not based on a demand strategy in all case study organizations. As a consequence, information security was often used too heavily (costly) within the IT organization.*

Research finding 6 *All case study organizations made information security investments decisions in an economic-independent way. Instead of conducting economic evaluations to justify the selected information mitigation solutions, within the case study organizations solutions were selected based on expert judgment and intuition.*

Research finding 7 *A lack of relevant content within all case study organizations resulted in the fact, that not all steps of the method could be done. For example, relevant past experience, statistical data and results of earlier inspections were lacking in these organizations.*

Research finding 8 *It was difficult to assess the cost-effectiveness of the mitigation solutions due to unavailability of the relevant content. So, it was hard to evaluate information security from an economic perspective.*

Research finding 9 *All case studies indicated that the proposed method was clear and complete. The method's steps were clear en logical. In addition, the method resulted in a better focus, analysis and argumentation.*

Research finding 10 *The method could be implemented and it could increase the organization's understanding of the economic evaluation of information security. However,*

organizations should meet some conditions to use the method and to evaluate information security from an economic perspective.

8.7 Answers to the research questions

The answers to the research questions stated in Section 1.8.1 are qualified with respect to the observations made during the research. Based on the findings of the literature study, the practice study, the expert review and the case studies, the following conclusions can be drawn.

Question 1: *Is it possible to design a method through which investments in information security are made in an adequate, economically grounded way?*

Based on literature study and practice study, a method was proposed to assist business management and IT management in information security investment decisions. The proposed method consists of the following three elements: *context*, *content* and *process* (see Section 8.5).

Question 2: *What are the contextual parameters to arrive at more economically grounded investments in information security?*

Summarized, the workability of the method can only be adequate, and information security can only be evaluated from an economic perspective under the following most important conditions:

- *The information security maturity level is sufficiently high (maturity level 4 and/or 5).* Metrics for information security management are measured, collected and communicated. The preceding does not suggest that the method is only applicable in organizations with a maturity level of 4 or 5. The method can also be applied in organizations with maturity levels 1, 2 or 3. However, at these lower maturity levels less relevant content exists to perform the economic evaluation in an adequate manner.
- *Business information security alignment.* Organizations have been addressing information security. However, the focus has been within the scope of an IT department. Information security needs to become part of the business. Organizations should include information security on business management's agenda.
- *Support for the method exists at the business management level and in the IT departments.* The success of every method, including the proposed one, depends on how it is employed and lived up to.
- *Relevant content is available.* Organizations should define/select and collect data on their information security risks, and to use measurement tools where this is possible and appropriate.
- *Sufficient time available to do economic judgments of information security.* If no time is available for preparing and conducting economic evaluations of information security (e.g. under pressure of regulations), then no time will be spent on economic evaluations.

- *Education of the personnel*. Personnel involved in the economic evaluation of information security investments must have knowledge of information security and investment economics.

Question 3: *What data is required to enable the economic evaluation of information security?*
Organizations should define/select and collect data on their security risks (see Section 4.3), and use measurement tools where this is possible and appropriate to estimate such data to obtain reliable input for the method.
Infromation security metrics provide a practical approach to measuring information security. They facilitate decision making through collection, analysis and reporting of relevant performance data. The primary benefits associated with information security investments are the future 'cost savings' derived from the prevention of losses due to information security breaches. Thus, organizations need to estimate the potential losses from information security breaches in order to estimate the benefits derived from information security investments.

Question 4: *Which process and which process steps should the data undergo to arrive at an economically grounded information security (investment) statement?*

The raw data undergo the following four core *steps*:
- Business Impact Analysis (BIA);
- Risk Analysis (RA);
- Risk Mitigation (RM); and
- On-going Effectiveness Evaluation (OEE).

The objective of the Business Impact Analysis is to obtain a risk rating for the information asset and to use it to decide upon the amount of resources to be invested so as to protect the asset from potential security breaches. There are several good reasons to do a Business Impact Analysis for the asset. First, not all assets have the same value to the business processes and thus to the organization. Some assets are so valuable that their loss could create a significant problem for the organization, for example by creating public embarrassment. Second, by focusing the security controls on the information areas that need them the most, the organization achieves a more efficient cost-to-benefit ratio.

The Risk Analysis, which builds upon the Business Impact Analysis, is performed to identify threats to the asset, vulnerabilities that could be exploited, losses that could result from an attack, and the likelihood of threat occurrence.
The process of Risk Mitigation is to strategically invest limited resources to change unacceptable risks into acceptable ones. Risk Mitigation involves the identification and implementation of cost-effective security controls to mitigate, control and resolve the organization's risks.

During the on-going effectiveness evaluation, actual effectiveness of implemented security controls is evaluated.

Question 5: *Is the method workable?*
The workability validation of the method has been performed in two activities, which are: expert reviews and three case studies. The case studies were performed within three Dutch

organizations. Professionals from different disciplines (business and IT) of each organization were invited to validate the workability of the method in one or more workshops.
In this thesis, workability was researched by finding answers to the following questions:

a. *Is the method clear and is the sequence of the steps logical?*
b. *Does relevant content exists within the organization to execute the process?*
c. *Are the results acceptable and good to take decisions?*

Ad a) All case studies indicated that the proposed method was clear and complete. The method's steps were clear and logical. In addition, the method resulted in a better focus, analysis and argumentation. The method wass, according to the participants, complete in its coverage of information security. It produced clear (trade-off) results, especially in comparing alternate security controls.

Ad b) Relevant content within the case study organizations was not available to evaluate information security from an economic perspective. A lack of relevant content resulted in the fact, that not all steps could be done. For example, relevant past experience, statistical data and results of earlier inspections were lacking in these organizations. There were also no standardized methods for determining the Risk Mitigation effectiveness of mitigation solutions, expressed in a value. Furthermore, the available content present in case study organizations was fragmented in the organization and not anchored into the process.

Ad c) This question could not be answered for the economic evaluation of information security investment. A lack of relevant content within the case study organizations resulted in the fact, that not all steps could be done, such as the economic evaluation of the proposed mitigation solutions. However, according to the participants, when relevant content within organizations would be available, the results of the method would be acceptable to business management. For example the money spent on the recommended security controls would be justifiable. Business management would understand why a particular security control had been recommended.

Central question: *How can investments in information security be made in an adequate, economically grounded way?*

The idea that information security has anything to do with economics is relatively new. As indicated by the case studies, organizations make information security investments decisions in an economic-independent way. The method proposed in see Chapter 4 could increase the organization's understanding of the economic evaluation of information security. This increased understanding could result in cost reductions, benefit maximization and improved decisions on costs of information mitigation solutions. However, the organizations should meet some conditions (see question 2) to use the method and to evaluate information security from an economic perspective.

8.8 Recommendations

Summarized, the research findings lead to the following recommendations to organizations, wishing to proceed with the economic evaluation of information security:

1. Determine at which information security maturity level the organization wants to arrive, and how that level can be reached. Metrics for information security should be defined, measured, collected and communicated. Information security requires security measurement in order to generate the feedback necessary.
2. Review the methods used within the organization to obtain the relevant content. Investigate how tooling can be used to record the relevant content. Organizations should collect information security incidents data prior to and post implementation of the security control, as well as the related business loss and cost data.
3. Involve business management in information security. Information security should not be viewed as an IT issue only, but as an integral part of the organization. Business management support may take the form of guidance during planning, participation during design, or involvement during deployment.
4. Reserve sufficient time to do economic judgments of information security and conduct training sessions. Initiate an effort to establish training sessions for employees/management on how to apply economics to information security investment decisions.